

IN THE CLAIMS

1 (Previously Presented). A method comprising:
disabling an operation of a wireless device that fails to communicate with a base station over a range limited wireless protocol.

2 (Previously Presented). The method of claim 1 including sending a short-range wireless signal from said wireless device to said base station.

3 (Previously Presented). The method of claim 2 wherein sending a short range wireless signal includes sending a Bluetooth protocol signal.

4 (Original). The method of claim 1 wherein preventing operation of the device includes preventing access to a supply of power.

5 (Previously Presented). The method of claim 1 including sending a wireless signal from said wireless device to a key fob.

Claim 6 (Canceled).

7 (Previously Presented). The method of claim 1 including preventing operation of the device if the signal is not authenticated by said base station.

8 (Previously Presented). The method of claim 1 including adversely affecting the performance of the device if the signal is not authenticated by said base station.

9 (Previously Presented). The method of claim 1 including limiting access to storage if the signal is not authenticated by said base station.

10 (Previously Presented). The method of claim 1 including preventing the device from booting if the signal is not authenticated by said base station.

11 (Previously Presented). A portable wireless device comprising:
a processor;
a wireless receiver; and
a storage coupled to said processor, said storage storing instructions that enable the processor to disable an operation of a wireless device that fails to communicate with a base station over a range limited wireless protocol.

12 (Previously Presented). The device of claim 11 wherein said receiver receives a short-range wireless signal.

13 (Previously Presented). The device of claim 12 wherein said receiver is a Bluetooth protocol transceiver.

14 (Previously Presented). The device of claim 11 wherein said processor to prevent operation of the device by preventing access to a supply of power.

15 (Previously Presented). The device of claim 11 wherein said device is in the form of a key fob.

16 (Previously Presented). The device of claim 11 to prevent operation of the device if the device sending a wireless signal is not authenticated.

17 (Previously Presented). The device of claim 11 wherein said device adversely affects the performance of the device if the signal is not authenticated.

18 (Previously Presented). The device of claim 11 wherein said device limits access to storage if the signal is not authenticated.

19 (Previously Presented). The device of claim 11 wherein said device prevents the device from booting if the signal is not authenticated.

20 (Previously Presented). An article comprising a medium storing instructions that enable a processor-based system to:

send a wireless signal from a portable device to a base station; and

disable an operation of the device that fails to communicate with a base station over a range limited wireless protocol.

21 (Original). The article of claim 20 further storing instructions that enable the processor-based system to receive a short-range wireless signal.

22 (Original). The article of claim 21 further storing instructions that enable the processor-based system to receive a Bluetooth protocol signal.

23 (Original). The article of claim 20 further storing instructions that enable the processor-based system to prevent access to a supply of power.

24 (Original). The article of claim 20 further storing instructions that enable the processor-based system to receive a wireless signal at a key fob.

25 (Original). The article of claim 20 further storing instructions that enable the processor-based system to receive a wireless signal at a concealed location.

26 (Original). An article of claim 20 further storing instructions that enable the processor-based system to prevent operation of the device if the signal is not authenticated.

27 (Original). An article of claim 20 further storing instructions that enable the processor-based system to adversely affect the performance of the device if the signal is not authenticated.

28 (Original). An article of claim 20 further storing instructions that enable the processor-based system to limit access to storage if the signal is not authenticated.

29 (Original). An article of claim 20 further storing instructions that enable the processor-based system to prevent the device from booting if the signal is not authenticated.